CLAIMS

What is claimed is:

1. A method of reporting malware events comprising the steps of:

detecting a malware event;

determining a level of the detected malware event;

comparing the level of the detected malware event to an event trigger threshold; and

transmitting a notification of the detected malware event, based on the comparison of the level of the detected malware event to the event trigger threshold.

2. The method of claim 1, wherein the detecting step comprises the step of:

detecting the malware event using a malware scanner.

3. The method of claim 2, wherein the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of a malware, or failure of a response to a malware.

4. The method of claim 1, wherein the malware event has one of a plurality of levels.

5. The method of claim 4, wherein the level of the malware event comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

6. The method of claim 5, wherein the event trigger threshold comprises one of a plurality of levels.

7. The method of claim 6, wherein the level of the event trigger threshold comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events

that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

8. The method of claim 7, wherein the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of a malware, or failure of a response to a malware.

9. The method of claim 1, wherein the transmitting step comprises the steps of:

transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and

transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold.

10. The method of claim 9, wherein the malware event has one of a plurality of levels.

11. The method of claim 10, wherein the level of the malware event comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

12. The method of claim 11, wherein the event trigger threshold comprises one of a plurality of levels.

13. The method of claim 12, wherein the level of the event trigger threshold comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

14. The method of claim 13, wherein the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of a malware, or failure of a response to a malware.

15. The method of claim 14, wherein the detecting step comprises the step of:

detecting the malware event using a malware scanner.

16. The method of claim 15, wherein the method further comprises the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

17. A system for reporting malware events comprising:

a processor operable to execute computer program instructions;

a memory operable to store computer program instructions executable by the processor; and

computer program instructions stored in the memory and executable to perform the steps of:

detecting a malware event;

determining a level of the detected malware event;

comparing the level of the detected malware event to an event trigger threshold; and

transmitting a notification of the detected malware event, based on the comparison of the level of the detected malware event to the event trigger threshold.

18. The system of claim 17, wherein the detecting step comprises the step of:

detecting the malware event using a malware scanner.

19. The system of claim 18, wherein the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of a malware, or failure of a response to a malware.

20. The system of claim 17, wherein the malware event has one of a plurality of levels.

21. The system of claim 20, wherein the level of the malware event comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

22. The system of claim 21, wherein the event trigger threshold comprises one of a plurality of levels.

23. The system of claim 22, wherein the level of the event trigger threshold comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events

that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

24. The system of claim 23, wherein the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of a malware, or failure of a response to a malware.

25. The system of claim 17, wherein the transmitting step comprises the steps of:

transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and

transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold.

26. The system of claim 25, wherein the malware event has one of a plurality of levels.

27. The system of claim 26, wherein the level of the malware event comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

28. The system of claim 27, wherein the event trigger threshold comprises one of a plurality of levels.

29. The system of claim 28, wherein the level of the event trigger threshold comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

30. The system of claim 29, wherein the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of a malware, or failure of a response to a malware.

31. The system of claim 30, wherein the detecting step comprises the step of:

detecting the malware event using a malware scanner.

32. The system of claim 31, further comprising the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

33. A computer program product for reporting malware events, comprising:

a computer readable medium;

computer program instructions, recorded on the computer readable medium, executable by a processor, for performing the steps of

detecting a malware event;

determining a level of the detected malware event;

comparing the level of the detected malware event to an event trigger threshold; and

transmitting a notification of the detected malware event, based on the comparison of the level of the detected malware event to the event trigger threshold.

34. The computer program product of claim 33, wherein the detecting step comprises the step of:

detecting the malware event using a malware scanner.

35. The computer program product of claim 34, wherein the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of a malware, or failure of a response to a malware.

36. The computer program product of claim 33, wherein the malware event has one of a plurality of levels.

37. The computer program product of claim 36, wherein the level of the malware event comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

38. The computer program product of claim 37, wherein the event trigger threshold comprises one of a plurality of levels.

39. The computer program product of claim 38, wherein the level of the event trigger threshold comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

40. The computer program product of claim 39, wherein the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of a malware, or failure of a response to a malware.

41. The computer program product of claim 33, wherein the transmitting step comprises the steps of:

transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and

transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold.

42. The computer program product of claim 41, wherein the malware event has one of a plurality of levels.

43. The computer program product of claim 42, wherein the level of the malware event comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

44. The computer program product of claim 43, wherein the event trigger threshold comprises one of a plurality of levels.

45. The computer program product of claim 44, wherein the level of the event trigger threshold comprises one of:

informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

46. The computer program product of claim 45, wherein the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of a malware, or failure of a response to a malware.

47. The computer program product of claim 46, wherein the detecting step comprises the step of:

detecting the malware event using a malware scanner.

48. The computer program product of claim 47, further comprising the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.